# Talos Incident Response

## El panorama dinámico de amenazas de la actualidad

El panorama de amenazas se ha convertido en un entorno complejo y desafiante para las organizaciones en todas partes. Esta escasez de talentos, combinada con un aumento en los incidentes, ha generado un estado de seguridad que suele ser débil en la mayoría de las organizaciones. Los defensores están acorralados. Las organizaciones de todo el mundo ahora se dan cuenta de que sentarse a esperar una alerta en su entorno conlleva multas severas, un mayor escrutinio, pérdida de propiedad intelectual, preocupaciones por la privacidad de los datos y pérdida de actividad comercial.

Para centrarse en el crecimiento y sus clientes, debe comenzar desde una base segura. La asociación con un servicio de respuesta ante incidentes se ha vuelto obligatoria para proteger los recursos, mitigar los riesgos y mantener el cumplimiento. Debe protegerse contra lo desconocido mediante la planificación y la experiencia proactivas para coordinar y llevar a cabo una respuesta.

## Mayor protección con Talos Incident Response

Talos Incident Response brinda un nuevo enfoque, capitalizando nuestra visibilidad inigualable, la inteligencia de amenazas única y procesable y la capacidad de respuesta colectiva y global, en conjunto en una oferta de espectro completo. Nuestros clientes no solo comprenden mejor sus capacidades de respuesta, sino que cuentan con la mayor inteligencia de amenazas, investigación y equipo de respuesta en el mundo de guardia cuando más importa. Ofrecemos un conjunto completo de servicios proactivos y reactivos para ayudarlo a prepararse, responder y recuperarse de una intrusión.



## Beneficios

- **Mayor visibilidad:** acceso al mayor conjunto combinado de telemetría, trampas de amenazas y datos Intel del Partner disponibles en cualquier lugar.
- **Inteligencia de amenazas procesable:** servicios mejorados basados en las últimas campañas de malware y notificaciones actualizadas y procesables sobre amenazas emergentes.
- **Respuesta más rápida:** la combinación de la respuesta ante incidentes de clase mundial y la capacidad de inteligencia de amenazas acelera la resolución de incidentes.
- **Acceso completo a las herramientas de Cisco** durante un incidente, para proporcionar una comprensión más amplia de todas las amenazas en la red.

# Caso de estudio

## Empresa de servicios de salud: escalamiento del ransomware a Cisco

### Desafíos

- Compromiso continuo de las credenciales de usuario por el agente de amenazas mediante correos electrónicos especialmente diseñados, admitidos por páginas web fraudulentas.

### Solución

- Los respondedores de Talos Incident Response definieron la línea de tiempo de ataque.
- Los respondedores implementaron AMP para terminales y Umbrella para ampliar la visibilidad en toda la empresa y ayudar a mitigar el ataque.
- Talos Incident Response y Cisco Email Security trabajaron en conjunto para implementar controles de seguridad para mitigar la recepción continua de correos electrónicos maliciosos.

### Resultado

- El cliente se recuperó rápidamente y pudo mitigar los ataques continuos gracias a la implementación de tecnologías adicionales y la orientación de los respondedores.
- El peso total de Cisco desde Talos Incident Response, el equipo de Cisco Email Security Appliance y la implementación de AMP para terminales y Umbrella, detuvieron la campaña de correo electrónico malicioso en curso.
- Los cambios a largo plazo en las configuraciones recomendadas por los respondedores de Talos Incident Response como la autenticación de varios factores, tendrán una mejora duradera en la postura de seguridad.

## Servicio Talos Incident Response: lo que se incluye

Talos Incident Response brinda los siguientes servicios:

- **Servicios de emergencia:** en caso de una intrusión, Talos estará disponible en cuestión de horas para clasificar, coordinar, investigar, contener, corregir y ayudar con comunicaciones de intrusiones.
- **Evaluación de la preparación de respuesta ante incidentes:** evaluamos varios puntos de datos, incluidos incidentes anteriores, roles y responsabilidades actuales, diseño de la organización, operaciones de parches, capacidades de registro y más para personalizar las recomendaciones para su entorno.
- **Estrategia y planificación:** los respondedores experimentados desarrollan una hoja de ruta y los planes asociados para saber cómo responder a los incidentes.
- **Ejercicio de simulación:** descubra las brechas en las políticas, los procedimientos y los procesos, y comprenda las actividades de comunicaciones importantes en este ejercicio interactivo.
- **Búsqueda proactiva de amenazas:** revisión proactiva de datos para buscar señales de ataque que pudieron haber evadido la detección anterior. Nos centramos en encontrar evidencia de la fase posterior a las vulnerabilidades en la cadena de eliminación.
- **Evaluación de riesgos:** una evaluación integral de la organización que busca indicadores de riesgo o de agentes de amenazas presentes en el entorno.
- **Cyber Range:** taller de capacitación técnica especializada para ayudar a su personal de seguridad a desarrollar las habilidades y la experiencia necesarias para combatir las ciberamenazas modernas.
- **Información a pedido:** consultas remotas completas o de medio día con los expertos de Talos para abordar las principales inquietudes de seguridad, las recomendaciones y el uso compartido de inteligencia para mejorar su postura general de seguridad.

## Próximos pasos

Visite Talos Incident Response para conectarse con nuestros respondedores y proteger su empresa hoy mismo.